Amendments to the Claims

Please amend the claims as follows:

1-81. (cancelled).

82. (currently amended) A [The] method of [claim 81 wherein] conducting an electronic transaction using an electronic card having a public key of a service provider, comprising:

formatting a key exchange request message at a member, the key exchange request message having [includes] a public key of the member, and at least a portion of the key exchange request message being encrypted using the service provider's public key from the electronic card;

sending the key exchange request message from the member to the service provider;

generating a session key exclusively at the service provider in response to the key exchange request message;

formatting a key exchange response message including the session key at the service provider;

sending the key exchange response message from the service provider to the member; and

using the session key to complete the transaction.

83. (previously added) The method of claim 82 wherein the key exchange request message further includes a member challenge for the service provider, and the key exchange response message further includes a response to the member challenge and a service provider challenge for the member, the method further comprising formatting by the member a response to the service provider challenge and sending it to the service provider.

84. (previously amended) The method of claim 82 or 83 wherein the use of the session key to complete the transaction comprises:

formatting by the member a transaction request message using the session key, the transaction request message including a digital signature of the member, and sending the transaction request message to the service provider; and

formatting at the service provider, a transaction response message for the member using the session key, the transaction response including a digital signature of the service provider, and sending the transaction response message to the member.

85. (previously added) The method of claim 84 wherein the transaction request message includes account information, transaction amount and transaction data, and wherein the formatting of the transaction request message by the member comprises encrypting with the session key the account information, the transaction amount and a portion of the transaction data.

86. (previously added) The method of claim 84 wherein the transaction request message comprises plain text.

87. (previously added) The method of claim 84 wherein the transaction request message comprises a transaction identification assigned to the member by the service provider.

88. (previously amended) The method of claim 84 wherein the transaction request message comprises the response to the service provider challenge.

89. (previously amended) The method of claim 84 wherein the transaction response message includes data encrypted with the session key.

90. (previously added) The method of claim 84 wherein the transaction response message includes plain text.

91. (previously added) The method of claim 84 wherein the transaction response message includes a transaction identifier assigned by the service provider to the member.

92. (previously added) The method of claim 84 further comprising formatting at the member, using the session key, a transaction acknowledgment message, digitally signing by the member the transaction acknowledgment message, and sending the transaction acknowledgment message to the service provider.

93. (previously added) The method of claim 92 wherein the transaction acknowledgement message includes data encrypted with the session key.

94. (previously added) The method of claim 92 wherein the transaction acknowledgement message includes plain text.

95. (previously added) The method of claim 92 wherein the transaction acknowledgement message includes a transaction identifier assigned to the member by the service provider.

96. (currently amended) A method of conducting an electronic transaction using an electronic card having a public key of a service provider, comprising:

generating a member challenge by a member;

encrypting by the member the member challenge using the service provider's public key from the electronic card to generate a first cryptogram;

formatting by the member a key exchange request message including the first cryptogram and a public key of the member;

signing digitally by the member the key exchange request message;

sending the digitally signed key exchange request message from the member to the service provider;

generating by the service provider a service provider challenge;

generating exclusively by the service provider a session key;

encrypting by the service provider the service provider challenge and the session key using the member's public key to generate a second cryptogram;

formatting by the service provider a key exchange response message including the second cryptogram and a response to the member challenge;

signing digitally by the service provider the key exchange response message;

sending the digitally signed key exchange response message to the member;

encrypting by the member a member response for the service provider challenge using the session key to generate a third cryptogram;

attaching the third cryptogram to a transaction message going from the member to the service provider;

signing digitally by the member the transaction message going from the member to the service provider; and

sending the transaction message from the member to the service provider.

97. (previously added) The method of claim 96 wherein the key exchange request message and key exchange response message each comprises plain text.

98. (previously amended) The method of claim 96 wherein the key exchange request message comprises the member's public key encrypted with the service provider's public key.

99. (previously amended) The method of claim 96 wherein the generation of the second cryptogram further comprises encrypting the member challenge response as part of the second cryptogram.

100. (previously added) The method of claim 96 wherein the generation of the second cryptogram further comprises encrypting a transaction identifier as part of the second cryptogram.

101. (previously added) The method of claim 96 wherein the key exchange response message further includes a transaction identifier comprising plain text.

102. (previously amended) The method of claim 101 further comprising using the transaction identifier with a second transaction message following the transaction message and going from the member to the service provider.

103. (previously amended) A method of communication using an electronic card having a public key of a service provider, comprising:

formatting a first key exchange request message at a first member, the first key exchange request message having a public key of the first member, and at least a portion of the first key exchange request message being encrypted using the service provider's public key from the electronic card;

sending the first key exchange request message from the first member to a second member;

combining at a second member, a second member key exchange request message with the first member's key exchange request message and sending the combined key exchange request message, signed by the second member, to a service provider;

generating a first session key exclusively by the service provider in response to the first key exchange request message;

generating a second session key exclusively by the service provider in response to the second key exchange request message;

formatting a key exchange response message at the service provider including a first session key for the first member, signing the response message, formatting a key exchange response message including the second session key for the second member, combining the key exchange response messages into a combined key exchange response message, signing the

combined key exchange response message, and sending the combined key exchange response message to the second member; and

separating at the second member, the key exchange response message for the second member from the key exchange response message for the first member, and forwarding the key exchange response message for the first member to the first member.

104. (previously added) The method of claim 103 further comprising:

formatting by the first member, using the first session key, a transaction request message, signing the transaction request message, and sending the transaction request message to the second member;

formatting by the second member, using the second session key, a transaction request message;

combining by the second member, the second member transaction request message with the first member transaction request message, signing the combined transaction request message, and sending the combined transaction request message to the service provider;

formatting by the service provider, using the first session key, a transaction response message for the first member, and signing the transaction response message;

formatting by the service provider, using the second session key, a transaction response message for the second member;

combining the transaction response message for the first member with the transaction response message for the second member to form a combined transaction response message, and signing the combined transaction response message;

sending the combined transaction response message to the second member;

separating at the second member, the transaction response message for the first member from the transaction response message for the second member; and

forwarding by the second member the transaction response message for the first member to the first member.

105. (previously added) The method of claim 104 further comprising:

formatting at the first member, using the first session key, an acknowledgment message, signing the acknowledgment message, and sending the acknowledgment message to a second member; and

formatting at the second member, using the second session key, an acknowledgment message, combining the second member acknowledgment message with the first member acknowledgment message to form a combined acknowledgment message, signing the combined acknowledgment message, and sending the combined acknowledgment message to the service provider.

106. (previously added) The method of claim 103 wherein the first session key is different from the second session key.

107. (previously added) The method of claim 103 wherein the first session key is the same as the second session key.

108. (previously added) The method of claim 103 wherein the key exchange response message for the second member includes the public key of the first member, and the key exchange response message for the first member includes the public key of the second member.

109. (previously amended) A method of communication using an electronic card having a public key of a service provider, comprising:

formatting a first key exchange request message at a first member, the first key exchange request message having a public key of the first member, and at least a portion of the first key exchange request message being encrypted using the service provider's public key from the electronic card;

sending the first key exchange request message from the first member to at least one intermediate member coupled in series between the first member and the service provider, each of said at least one intermediate member being either a message router or a participating member;

generating, if said at least one intermediate member comprises at least one participating member, at each of the participating members a key exchange request;

receiving at the service provider a combined key exchange request message from said at least one intermediate member, the combined key exchange request message comprising the first key exchange request message and the key exchange request message generated by each of the participating members;

generating exclusively by the service provider a first session key for the first member and a participating session key for each of the participating members;

formatting at the service provider a key exchange response message including each of the first and participating session keys;

sending the key exchange response message from the service provider to said at least one intermediate member;

separating by each participating member its respective participating session key from the key exchange response message; and

sending the first session key from said at least one intermediate member to the first member.

110. (previously added) The method of claim 109 further comprising:

encrypting a first transaction request message using the first session key at the first member;

sending the first transaction request message from the first member to said at least one intermediate member;

generating, if said at least one intermediate member comprises at least one participating member, at each of the participating members a transaction request message encrypted using its respective participating session key;

receiving at the service provider a combined transaction request message from said at least one intermediate member, the combined transaction request message comprising the first transaction request message and the transaction request message for each of the participating members;

formatting at the service provider a combined transaction response message comprising a transaction response message for the first member and each of the participating members;

sending the combined transaction response message from the service provider to said at least one intermediate member;

separating by each participating member its respective transaction response message from the combined transaction response message; and

sending the transaction response message for the first member from said at least one intermediate member to the first member.

111. (previously added) The method of claim 109 wherein the first session key and the participating session keys are each different from one another.

112. (previously added) The method of claim 109 wherein the first session key and the participating session keys are the same as each other.

113. (previously amended) A method of communication using an electronic card having a public key of a service provider, comprising:

formatting a key exchange request message at each of a plurality of first members, the key exchange request message for one of the first members having a public key of said one of the first members, and at least a portion of the key exchange request message for said one of the first members being encrypted using the service provider's public key from the electronic card;

sending from each of the first members its respective key exchange request message to a second member, the second member being either a message router or a participating member;

generating, if the second member is a participating member, a second key exchange request message at the second member;

combining at the second member the key exchange request message from each of the first members to form a combined key exchange request message, the combined key exchange request message further comprising the second key exchange request message if the second member is a participating member;

receiving at the service provider the combined key exchange request message from the second member;

generating exclusively by the service provider a first session key for each of the first members, and a second session key for the second member if the second member is a participating member;

formatting at the service provider a key exchange response message including each of the first and second session keys;

sending the key exchange response message from the service provider to the second member;

separating by the second member the second session key from the key exchange response message if the second member is a participating member;

separating by the second member the first session key for each of the first members from the key exchange response message; and

sending each of the first session keys to its respective first member.

114. (previously added) The method of claim 113 further comprising:

encrypting a transaction request message at each of the first members using their respective first session keys;

sending from each of the first members its respective transaction request message to the second member;

generating, if the second member is a participating member, a second transaction request message at the second member and encrypting the second transaction request message with the second session key;

combining at the second member the transaction request message from each of the first members to form a combined transaction request message, the combined transaction request message further comprising the second transaction request message if the second member is a participating member;

receiving at the service provider the combined transaction request message from the second member;

generating at the service provider a transaction response message for each of the first members, and the second member if the second member is a participating member;

formatting at the service provider a combined transaction response message including the transaction response messages for each of the first members, and the second member if the second member is a participating member;

sending the combined transaction response message from the service provider to the second member;

separating by the second member its respective transaction response message from the combined transaction response message if the second member is a participating member;

separating by the second member the transaction response messages for each of the first members from the combined transaction response message; and

sending each of the transaction response messages to its respective first member.

115. (previously added) The method of claim 113 wherein the first session keys and the second session key are each different from one another.

116. (previously added) The method of claim 113 wherein the first session keys and the second session key are the same as each other.